REMARKS

This amendment is responsive to the Office Action dated February 11, 2005. Applicants have amended claims 1, 5, 7, 8, 12, 13, 20-23 and 30. Claims 1-30 remain pending.

Claim Rejection Under 35 U.S.C. § 112

In the Office Action, the Examiner rejected claim 13 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. Applicants have amended claim 13 for purposes of clarification. Applicants submit that claim 13, as amended, particularly points out and distinctly claims the subject matter, as required by 35 U.S.C. 112, second paragraph. Applicants request withdrawal of the rejection under 35 U.S.C. 112, second paragraph.

Claim Rejection Under 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 1-4, 6-9, 12-15, 18-21 and 23-30 under 35 U.S.C. 102(e) as being anticipated by Jardin (USPN 6,681,327). Applicants respectfully traverse the rejection to the extent such rejection may be considered applicable to the amended claims. Jardin fails to disclose each and every feature of the claimed invention, as required by 35 U.S.C. 102(e), and provides no teaching that would have suggested the desirability of modification to include such features.

Claims 1-4, 6, 7, 12, 13, 15, 18-21 and 23-30

Applicants have amended independent claims 1, 12, 23 and 30 to clarify that, unlike conventional accelerators, the claimed intermediate device decrypts application data and forwards the application data to a server without processing the application data with an application layer of a network stack of the intermediate device. In other words, the application layer of the network stack of the intermediate device is effectively bypassed.

For purposes of clarity, Applicants refer the Examiner to Figure 2B and pages 5 and 6 that describe conventional SSL acceleration devices and, in particular, how in prior art systems HTTP packets conventionally traverse the entire networking protocol stack including the IP layer, the SSL session layer and the application layer multiple times. Although Jardin is relatively silent as to the actual exchange of application data between client and server via the broker, Jardin makes clear that "the broker 120 and server 130a are ready to exchange application data in conventional form."

In contrast to techniques applied by Jardin and conventional acceleration devices, embodiments of the present invention include an acceleration device that operates at the packet level. For purposes of illustration, Applicants refer the Examiner to page 10, ll. 3-13 of the present application that states:

> *Figure 3 shows how the system of the present invention differs in general from that of the prior art, and illustrates the manner in which the SSL encryption and decryption proxy is implemented. Typically, when a Web client wishes to send data via a secure protocol to an SSL enabled Web server, it will do so by communicating via a secure port 443. As shown in Figure 3, in accordance with the present invention, the SSL accelerator will intercept data destined for port 443 of the web server and, rather than the transmitting packets up and down the TCP/IP stack as shown in Figure 2B, will perform the SSL encryption and decryption at the packet level before forwarding the packet on to its destination. The accelerator will thus decode the packet data and forward a clear text (HTTP) packet the HTTP port 80 of the Web server 300.*

Further, on page 16, ll. 17-26, the present application states that:

> *As shown at reference number 265, client 100 will now begin sending encrypted application data to the SSL accelerator device 250. ... The accelerator device will process the data at step 270 on the packet level and forward it to the server as clear text.*

Thus, Jardin fails to teach or suggest decrypting encrypted application data with an intermediate device and forwarding decrypted application data from the intermediate device to the server via the secure network without processing the application data with an application layer of a TCP/IP stack, as required by claim 1 as amended. Again, Jardin states that application data is exchanged in a conventional manner and makes no mention of an intermediate device that decrypts packets and forwards the packets without processing the decrypted packet data with the application layer.

With respect to amended claim 23, Jardin fails to teach or suggest decrypting data packets of the secure protocol to provide decrypted packet data at the packet-level of a network stack of the intermediate device. Further, Jardin fails to teach or suggest bypassing an application layer of the network stack of the intermediate device and forwarding the decrypted packet data from the intermediate device to at least one server of the enterprise without processing the decrypted packet data with the application layer.

Similarly, with respect to amended claim 30, Jardin fails to teach or suggest bypassing an application layer of a network stack of the intermediate device and forwarding decrypted application data from the intermediate device to the server via the secure network without processing the decrypted packet data with the application layer.

For at least these reasons, the rejection of claims 1, 12, 23 and 30 under 35 U.S.C. 102(e) should be withdrawn.

Claims 8 and 14

Applicants' claims 8 and 14, as amended, require prior to establishing a communications session with one of said plurality of servers, selecting one of said plurality of servers to forward the decrypted authentication data to based on a load balancing algorithm that calculates processing loads associated with each of the servers.

With respect to claims 8 and 14, the Examiner relied on column 8, lines 27-67 through col. 9, line 10 of Jardin. In the cited portions, however, Jardin first describes a "broker 130" that re-directs an existing session to different severs if a server generates errors (col. 8, ll.27-41). Redirection of an existing session in response to errors is fundamentally different from actively load-balancing across the servers by selecting the server based on current processing loads prior to establishing the communication session with the selected server, as required by Applicants' claims 8 and 14.

The remainder of the cited portion of Jardin describes redirecting a transaction from one server to another if a response time for the original server exceeds a defined threshold. Again, redirection due to an inadequate response time is fundamentally different from actively load-balancing across the servers by selecting the server based on current processing loads prior to even establishing the communication session with the selected server, as required by Applicants' claims 8 and 14.

For at least these reasons, the rejection of claims 8 and 14 under 35 U.S.C. 102(e) should be withdrawn.

Claim Rejection Under 35 U.S.C. § 103

Claims 5 and 22

In the Office Action, the Examiner rejected claims 5 and 22 under 35 U.S.C. 103(a) as being unpatentable over Jardin in view of Narad (USPN 6,157,955). Applicants respectfully traverse the rejection to the extent such rejections may be considered applicable to the claims as amended. The applied references fail to disclose or suggest the inventions defined by Applicants' claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Applicants have amended claim 5 to require receiving the application data as multi-segment records, forwarding at least a portion of the decrypted application for each of the records prior to receiving complete records, discarding at least a portion of each of the records after forwarding, and authenticating the decrypted application data of each data record using the remaining non-discarded portion of the data record upon receiving a final segment of the multi-segment record.

Applicants have amended claim 22 to require discarding at least a portion of a multi-segment encrypted data record, and authenticating the decrypted data using the remaining portion of the data record after a final segment of the data record is received.

No new matter has been added by the amendments. Support for the amendments can be found throughout the specification, including from pg. 26, ln. 20 to pg. 27, ln. 20.

With respect to claims 5 and 22, the Examiner correctly acknowledges that Jardin fails to teach or suggest authenticating decrypted packet application data of a security record on receipt of a final packet of the security record. Nevertheless, the Examiner states that it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the Jardin system in view of the teachings of Narad to authenticate packet application data on receipt of a final packet of a segment.

In contrast to Applicants' amended claims 5 and 22, Narad describes a general-purpose packet processing system that includes a Policy Engine (PE) that applies policy decisions to packets based on the results of a packet Classification Engine (CE). Narad makes no mention of authenticating a security record or application data that spans multiple segments when receiving the final segment at all. The "cryptographic key" referenced by the Examiner is described by Narad in reference to a cryptographic unit that generally supports encryption and decryption. The "checksum" described by Narad is merely used to determine whether a packet is valid or corrupted in some form. Narad does not describe authenticating a security record or authenticating application data that spans multiple packets.

Consequently, neither Jardin nor Narad, either separately or in combination, teach or suggest discarding at least a portion of a multi-segment encrypted data record, and authenticating the decrypted data using the remaining portion of the data record after a final segment of the data record is received, as required by Applicants' amended claim 5 and 22.

For at least these reasons, the rejection of Applicants' claims 5 and 22 under 35 U.S.C. 103(a) should be withdrawn.

Claims 10, 11, 16 and 17

In the Office Action, the Examiner rejected claims 10, 11, 16 and 17 under 35 U.S.C. 103(a) as being unpatentable over Jardin in view of Abramson et al (USPN 6,539,494). Applicants respectfully traverse the rejection. Neither Jardin nor Abramson disclose or suggest the inventions defined by Applicants' claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

With respect to claims 10, 11, 16 and 17, the Examiner correctly acknowledges that Jardin fails to teach or suggest establishing a session tracking database recording, for each session, a session ID, a TCP sequence number and an SSL session number. Nevertheless, the Examiner states that it would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the Jardin system in view of the teachings of Abramson to include such requirements.

In contrast to Applicants' claims, Abramson describes a computer system for a web site that uses three tiers of servers: web (or HTTP) servers, application servers, and backup servers.[1] According to Abramson, the third tier of servers, i.e., the backup servers, is responsible for

[1] Abstract

backing up session data associated with the clients. Thus, Abramson is not referring to an intermediate proxy device, but the use of an entire new tier of backup servers. Moreover, Abramson is not describing SSL sessions or any other type of secure communication.

Consequently, neither Jardin nor Abramson, either separately or in combination, teach or suggest an intermediate device that tracks data passing between the client and the plurality of servers, as required by claims 10, 16 and 17.

Moreover, neither Jardin nor Abramson even mention storage of an initialization vector for each session, as required by claim 17. As described in the present application, initialization vectors relate to secure communication sessions using cryptographic keys. Abramson makes no mention of secure communication sessions, and fails to teach or suggest an intermediate device that maintains initialization vectors for secure communications between clients and servers. Thus, the Jardin system could not be modified in view of Abramson in a manner that achieves Applicant's invention as recited by claim 17.

For at least these reasons, the rejection of Applicants' claims 10, 11, 16 and 17 under 35 U.S.C. 103(a) should be withdrawn.

Provisional Rejection for Obviousness-type Double Patenting:

The Examiner rejected claims 1-7, 12, 15 and 19-30 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-20 of commonly owned copending Application No. 09/900,493. As indicated by the Examiner, this is a provisional rejection because none of the conflicting claims have in fact been patented. Applicants will address the rejection when formally applied.

CONCLUSION

All claims in this application are in condition for allowance. Applicants respectfully request reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date: May 9, 2005

By:

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312